



HM TREASURY



National Audit Office

GOOD
PRACTICE
GUIDE

Tackling external fraud



The National Audit Office scrutinises public spending on behalf of Parliament. The Comptroller and Auditor General, Tim Burr, is an Officer of the House of Commons. He is the head of the National Audit Office which employs some 850 staff. He and the National Audit Office are totally independent of Government. He certifies the accounts of all Government departments and a wide range of other public sector bodies; and he has statutory authority to report to Parliament on the economy, efficiency and effectiveness with which departments and other bodies have used their resources. Our work saves the taxpayer millions of pounds every year: at least £9 for every £1 spent running the Office.

Contents

| | |
|---|----|
| Foreword | 5 |
| Introduction | 6 |
| <hr/> | |
| Part 1: Understanding and managing the risks of fraud | 10 |
| Taking a strategic approach to tackling external fraud | 11 |
| Assessing the scale of the threat | 13 |
| Understanding the types of fraud risks | 16 |
| Focusing resources on the most effective anti-fraud measures | 17 |
| Setting targets and monitoring performance | 17 |
| Responsibilities for tackling fraud | 18 |
| <hr/> | |
| Part 2: Deterring and preventing external fraud | 20 |
| Changing public attitudes to fraud | 21 |
| Changing staff attitudes to create an anti-fraud culture | 23 |
| Controls to prevent fraud | 24 |
| Strengthening internal controls and checks | 26 |
| <hr/> | |
| Part 3: Detecting and investigating external fraud and imposing sanctions | 28 |
| Detecting fraud | 29 |
| Investigating cases of fraud | 33 |
| Imposing sanctions | 36 |
| The recovery of money defrauded | 39 |
| Evaluating the effectiveness of sanctions | 41 |
| Working with others in tackling fraud | 41 |

Foreword

Reports published by departments, HM Treasury, the National Audit Office and the Committee of Public Accounts show that much good work is being done across departments to prevent and detect fraud against public funds. But large sums of public money are still lost each year through external fraud. These losses arise from a wide range of different types of fraud. At one end of the scale are people who see an opportunity to make a small gain. At the other extreme a relatively small number of organised crime groups carry out premeditated systematic attacks for large sums of money. The law abiding public have the right to expect government departments and agencies to safeguard public funds and to crack down on those committing fraud.

All types of fraudsters weigh up the potential gains against the risk of getting caught and the sanctions they may face. Government departments and agencies need to make fraud as unattractive as they can. Not acting against fraud can undermine the reputation, integrity and professionalism of the organisation and perceptions about the quality of the services it provides leading to a loss in public confidence.

A number of departments are carrying out fraud risk assessments to show the scale of the problem and are assessing how these risks can be reduced. Total elimination of fraud is unlikely ever to be achieved, but it is important for momentum to be maintained, and good practices developed and shared.

The purpose of the guide is to demonstrate and explain some of the good practices used by organisations in tackling external fraud. It includes checklists to help you assess your current practices. The guide should be of interest to public sector managers who are responsible for expenditure programmes and for protecting revenue, including policy staff, financial managers and internal auditors. Smaller departments and agencies will need to consider how practices used in some of the larger departments can be adapted and applied to their own circumstances.

We are grateful for the help provided by the departments and other organisations in producing this guide.

John Kingman
Second Permanent Secretary
HM Treasury

Caroline Mawhood
Assistant Auditor General
National Audit Office

Introduction

1 This guide concentrates on external fraud which is where third parties, such as businesses, individuals or organised crime groups, steal money from a department or agency, either by obtaining payments to which they are not entitled or keeping monies they should pay over to the department. Frauds may be opportunistic attempts by individual customers or businesses to obtain a financial advantage. The sums involved in any one such case may be small, but these can mount up to significant losses of public money if there are a lot of cases involved. At the other end of the scale, departments or agencies may suffer from more systematic and premeditated attacks by organised crime groups. These may be fewer in number but the losses in each case are substantial. In some cases fraudsters may work in collusion with the department's staff. As well as diverting money that should be spent on public services fraud can undermine the position of honest citizens and businesses and support the activities of those involved in other serious crime.

2 The *Fraud Act 2006*¹ includes three classes of fraud:

- Fraud by false representation;
- Fraud by failing to disclose information;
- Fraud by abuse of position.

In all three classes of fraud, the Act requires that for an offence to have occurred, the person must have acted dishonestly, and that they had to have acted with the intent of making a gain for themselves or anyone else, or inflicting a loss (or risk of a loss) on another. There are also offences of fraud specific to particular departments' activities.

3 All government departments and agencies have a responsibility to develop anti-fraud policies to show those seeking to defraud the government that such action is unacceptable and will not be tolerated². The annual *Statement on Internal Control* summarises the processes used to identify and manage risks including fraud³. In addition the *Proceeds of Crime Act 2002*⁴, the *Money Laundering Regulations (2003*⁵, 2007⁶) and related legislation have placed responsibilities on regulated entities and every person carrying out "relevant business" within the meaning of the Regulations, to report where they know, or suspect, or have reasonable grounds to suspect, that money

¹ *Fraud Act 2006* – http://www.opsi.gov.uk/acts/acts2006/pdf/ukpga_20060035_en.pdf

² *Managing Public Money*, Annex 4.7 – http://documents.treasury.gov.uk/mpm/mpm_annex4.7.pdf

³ *Managing Public Money*, Annex 4.15 – http://documents.treasury.gov.uk/mpm/mpm_annex4.15.pdf

⁴ *Proceeds of Crime Act 2002* – <http://www.legislation.hmso.gov.uk/acts/acts2002/20020029.htm>

⁵ The Money Laundering Regulations 2003 (Statutory Instrument 2003, Number 3075) – <http://www.legislation.hmso.gov.uk/si/si2003/20033075.htm>

⁶ The Money Laundering Regulations 2007 (Statutory Instrument 2007, Number 2157) – http://www.hm-treasury.gov.uk/media/F/1/money_laundering_regulations2007.pdf

laundering may be taking place. Most government departments are not classified as “relevant businesses” but it is good practice to assess the risks and potential exposure; and, where appropriate, departments should regard themselves as “relevant businesses” and act accordingly. These reporting responsibilities also apply to the National Audit Office as external auditor. Money laundering involves not only the direct proceeds of crime, but any dealings with criminal property. It includes possessing, or in any way dealing with, or concealing, the proceeds of any crime. Any failure to report suspicions of money laundering is now a criminal offence. Regulated entities must take appropriate measures to ensure that key staff are aware of the provisions of the Act and the Regulations, and appoint a Money Laundering Reporting Officer to report their knowledge or suspicions to the Serious Organised Crime Agency.

4 In response to the Fraud Review of 2006⁷, the Government provided £29 million of new funding to implement its recommendations, including the setting up of:

- a National Fraud Strategic Authority – to define and co-ordinate delivery of a national strategy that sets out a vision of success in tackling fraud; the steps needed to realise it; and measuring the impact that these efforts are having.
- The Fraud Loss Measurement Unit of the National Fraud Strategic Authority – to provide robust estimates for repeat measurement of losses before and after action has been taken; and a strategic assessment of the risks and possible losses from future threats.
- The National Fraud Reporting Centre and Intelligence Bureau – to be the hub in which knowledge about fraud is collated and managed. It will provide an outward facing service to the public; the business community and police forces; receiving reports of fraud offences and incidents, adding intelligence and providing packages of analysed information to target investigations and other action. These may include criminal investigations conducted by the police, confiscation investigations or other forms of action taken by government departments, agencies or by industry.
- The National Lead Force for Fraud – to provide resources and support for police forces in tackling fraud. The City of London Police will take on the lead role.

5 Departments and agencies face a wide range of different risks from external fraud which are demonstrated in **Figure 1**. There are also many other types of fraud perpetrated by third parties, such as fraud by contractors. In some departments or agencies external fraud is a sizeable and continuing problem for their main business but in others it may only occur occasionally.

⁷ *Fraud Review Final Report*, July 2006 – <http://www.attorneygeneral.gov.uk/Fraud%20Review/Fraud%20Review%20Final%20Report%20July%202006.pdf>

Figure 1

The diversity of external frauds faced by the public sector

- Benefit claimants who fail to declare all earnings, income or capital, or who conceal family circumstances, to obtain benefits to which they are not entitled.
- People who claim exemption from paying for prescriptions to which they are not entitled.
- Dentists who claim for treatments which they have not carried out.
- People who evade vehicle excise duty.
- People or businesses who claim grants to which they know they are not entitled.
- People who work in the hidden economy and do not pay income tax or national insurance contributions on their earnings. They may also claim means tested benefits from the Department for Work and Pensions to which they are not entitled.
- People and businesses who register with HM Revenue & Customs but fail to declare all transactions/income or assets on which tax is due.
- Staff colluding with criminals to defraud the department or agency. For example in 2005 an employee in a department sold details of departmental records to an external accomplice to allow them to fraudulently claim £1.25 million of payments from the department.
- Serious criminals obtaining large sums, for example: through evading tobacco, alcohol and hydrocarbon oil duties; setting up what appear to be legitimate companies but intend to carry out frauds, such as to steal VAT; committing organised fraud against the benefit system through stolen, forged or counterfeit instruments of payment; or through creating fictitious benefit claims.

6 Departments should consider whether they need to develop a package of measures specifically tailored to each type of fraud. There will not be a “one size fits all” approach. But there is much value in promoting a wider understanding of how others tackle fraud and good practices which are successful elsewhere. Smaller departments and agencies should consider whether they can adapt and apply practices used by larger departments in tackling external fraud.

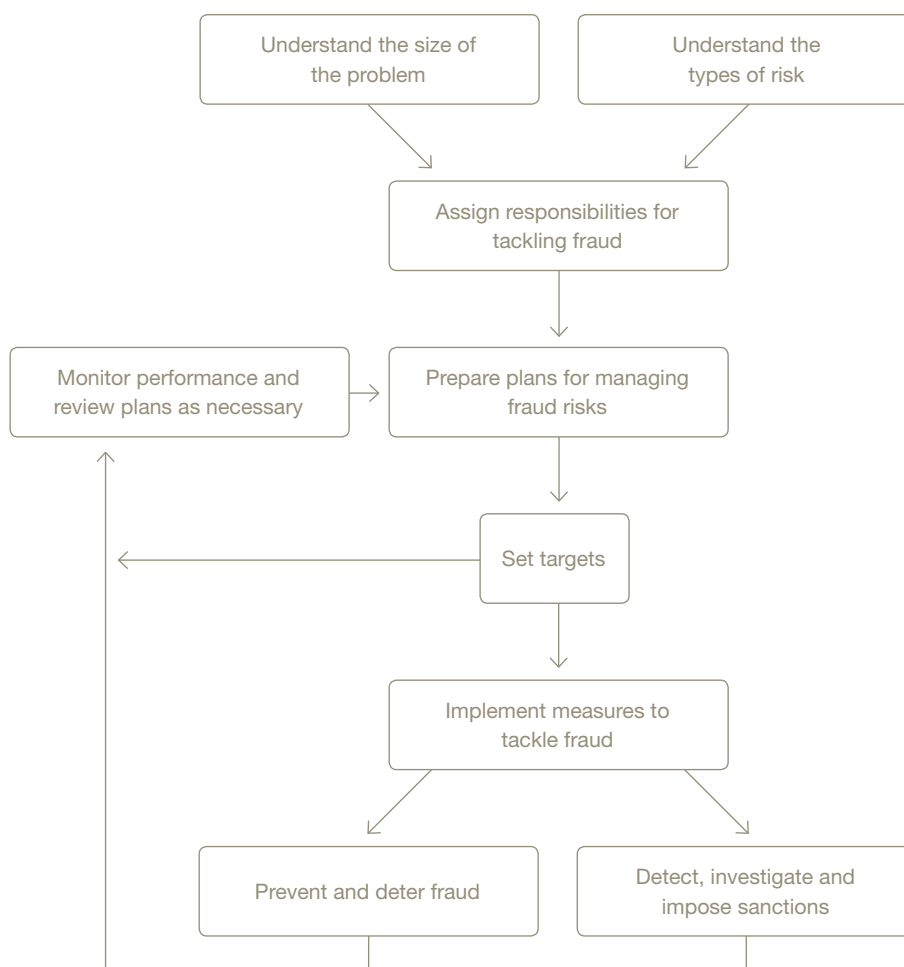
7 The guide shows how a number of departments are tackling fraud by taking an integrated strategic approach which is summarised in **Figure 2**. It also explains why they are taking this approach and what it involves. The strategic approach accords with the HM Treasury’s guidance *The Orange Book: Management of Risk*⁸ and *Managing the Risk of Fraud: A Guide for Managers*⁹ which provide guidance on the identification and management of risk, and guidance on controlling identified fraud risk to acceptable levels of exposure.

⁸ *The Orange Book: Management of Risk – Principles and Concepts*, HM Treasury, October 2004 <http://www.hm-treasury.gov.uk/media/3/5/FE66035B-BCDC-D4B3-11057A7707D2521F.pdf>

⁹ *Managing the Risks of Fraud: A guide for managers* – http://www.hm-treasury.gov.uk/media/C/3/managing_the_risk_fraud_guide_for_managers.pdf

Figure 2

The main elements of an integrated strategic approach to tackling fraud



8 The guide is structured as follows:

- Understanding and managing the risks of external fraud (Part 1);
- Preventing and deterring external fraud (Part 2);
- Detecting and investigating fraud and imposing sanctions (Part 3).

Questions at the beginning of each Part are to help you assess your organisation's practices. If you are not using a particular practice you will need to consider whether that is appropriate given your circumstances.

9 We hope that the guide is a useful source of reference for public sector managers in demonstrating the experience and good practice of others. It does not seek to provide “everything you need to know” to tackle external fraud. To do so would require many volumes. However, the guide provides references to useful sources of information and gives links to where these are available on websites. The case examples in the guide are for illustrative purposes only. There may be many other examples of good practice in other departments or agencies.

Part 1

Understanding and managing the risks of fraud

“NHS fraud is not a victimless crime. Every pound lost to fraud deprives the NHS of valuable resources it needs to provide patient care.”

Dermid McCausland, Managing Director, NHS Counter Fraud Service

In looking at this Part of the guide, ask yourself whether your organisation:

- takes a strategic approach to tackling fraud risk;
- assesses the size of the threat from external fraud and, where significant, undertakes a separate risk assessment;
- knows the size of the fraud threat/types of fraud committed/who is committing them/how often/and how much is involved;
- has a package of measures in place to tackle losses from fraud where these are significant;
- has targets to stabilise or reduce fraud;
- has allocated responsibilities for tackling, and ownership of, fraud risks to ensure that risks are managed, plans are implemented and progress monitored.

This Part of the guide looks at how you can tackle some of these issues and gives examples of how others approach these issues. As you read through the guide you will need to consider how appropriate the practices are to your circumstances.

Taking a strategic approach to tackling external fraud

“Protecting tax revenues is an essential part of the Government’s commitment to prosperity and fairness. Its strategy has delivered a major improvement in revenue collection over the last few years.”

Protecting tax revenues, HM Revenue & Customs strategy document, Budget Report 2008

1.1 Some organisations have taken a strategic approach to understanding and managing the risks of fraud because this:

- Fits in with good corporate governance.
A major element of good corporate governance is a sound assessment of the organisation’s business risks. Fraud risk should be managed in the same way as managing any other business risk and should therefore be approached systematically at both the organisational and operational level.
- Helps with developing a range of measures which apply proportionate and well targeted pressure at all levels of the problem.
- Can help achieve a cost effective approach in tackling fraud by focusing on areas of greatest risk and where efforts may have the greatest impact. A strategic approach can provide a rational and robust basis in bidding for additional resources to tackle fraud.
- Can be a helpful way of communicating to staff what the organisation is trying to do and what is expected from them. Some organisations have also published their strategies as a way of informing the public that they have a well thought out approach to tackling external fraud. This can also send a deterrent message to potential fraudsters that they are unlikely to succeed in attempts to commit fraud against the organisation. As examples, HM Revenue & Customs, the Department for Work and Pensions and the NHS Counter Fraud Service have published strategies.

Figure 3 shows examples of how departments and agencies have reduced external fraud and **Figure 4** provides the main elements of a strategy to tackle external frauds.

Figure 3

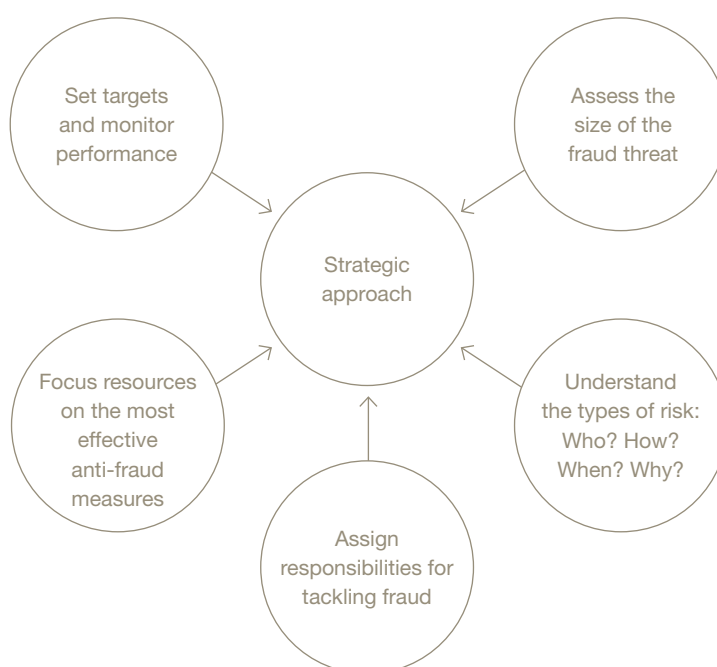
Examples of how external fraud has been reduced

In 2006-07 the **Department for Work and Pensions** estimated that fraud against Jobseeker’s Allowance, Income Support and Pension Credit has fallen from £900 million to £430 million since 1997-98 – a reduction of just over 50 per cent.

In the 2008 Budget report, **HM Revenue & Customs** estimated that the set of strategic measures introduced to protect revenues over the previous 5 years had reduced tax losses in priority areas – VAT, the main excises, the main direct taxes and National Insurance Contributions – by over £5 billion a year.

Figure 4

The main elements of a strategic approach to tackling external fraud



1.2 In taking a strategic approach, some departments and agencies have taken an across the board approach to looking at external fraud, and some have looked at individual fraud risks and produced a strategy for each. Others tackle fraud within the context of an overall strategy to combat losses from all types of non-compliance. The overall compliance approach recognises that there is a 'loss continuum' ranging from inadvertent customer error at one end of the spectrum to fraud at the other with shades of grey in between

All of these approaches can be equally valid depending on a department's circumstances and the stage they are at in developing their approach (Figure 5). However, a common feature is that the departments and agencies develop fraud risk assessment tools to identify the fraud risks, their likelihood and impacts, and how to manage them. These tools need to be reviewed regularly to assess whether they remain appropriate or require updating to respond to the threat from new fraud risks.

Figure 5
Examples of counter fraud strategies

| | | |
|--|---|---|
| <p>The Department for Work and Pensions has developed a counter fraud strategy for all welfare benefits. First set out in 1999, the strategy proposed action on four fronts:</p> <ul style="list-style-type: none">● Getting it right – aiming to get benefit payments correct from day one;● Keeping it right – ensuring payments are adjusted as circumstances change;● Putting it right – detecting when payments go wrong and taking prompt action to correct them with appropriate penalties to prevent a recurrence;● Making sure the strategy works – by monitoring progress, evaluating the strength of preventive measures and adjusting them in the light of experience. <p>The Department seeks to ensure that their goals of supporting people in their efforts to find work, whilst providing appropriate financial support where necessary, are not compromised by their efforts to prevent fraudulent abuse of the benefits system.</p> | <p>The NHS Counter Fraud Service's strategy consists of seven objectives:</p> <ul style="list-style-type: none">● the creation of an anti-fraud culture;● maximum deterrence of fraud;● successful prevention of fraud which cannot be deterred;● prompt detection of fraud which cannot be prevented;● professional investigation of detected fraud;● effective sanctions where fraud is proven;● redress for money defrauded. <p>HM Revenue and Customs' approach to tackling fraud has a number of key components:</p> <ul style="list-style-type: none">● the development of reliable estimates of the size of tax losses as far as possible; | <ul style="list-style-type: none">● establishing the nature and economics of the activity and behaviour that cause the losses, through the analysis of intelligence and other data;● a comprehensive set of responses based on:<ol style="list-style-type: none">1 Support: building services that are tailored to the needs and circumstances of taxpayers;2 Prevention: ensuring that basic processes and design make the system as secure as possible from fraud and avoidance;3 Identifying and tackling those who set out to obtain an unfair tax advantage: using improved risk assessment and checks, with sanctions as appropriate tailored to behaviour.● Monitoring effectiveness against key outcomes to measure the success of the strategies. |
|--|---|---|

Assessing the scale of the threat

“It will never be possible to measure 100 per cent of fraud; there will always remain undiscovered fraud. But better measurement is crucial to a properly designed and effective strategic response to fraud and to supporting better management of fraud risks.”

Fraud Review: Final Report

1.3 Assessing the scale of loss from fraud is an important first step in developing a strategy for tackling external fraud. An estimate highlights the scope for potential savings which can then help to determine the relative priority that should be given to tackling fraud in the context of all the other calls on an organisation's resources. Such estimates then establish a baseline against which performance can be judged. If repeated at intervals, estimates can help an organisation assess how well they are doing and whether the threat is changing. There may be circumstances where an organisation decides it is not practicable to produce overall estimates. Nevertheless they may be able to use a range of techniques such as carrying out in-depth research into an area where fraud is suspected to gain a better understanding of the scale and nature of the threat (**Figure 6**).

Figure 6

HM Revenue & Customs' approach to measuring taxpayer compliance

Where it is not possible to produce reliable estimates of the amount of tax lost to fraud HM Revenue & Customs may use the following techniques:

- audit based studies – random enquiry programmes to provide estimates of non-compliance and to facilitate research into understanding the risks of non-compliance in specific taxpayer and customer groups;
- modelling techniques applied to compliance data to explain or predict taxpayer non-compliance.

1.4 Some may say that:

- It is too difficult to produce estimates of fraud and that it is not worth attempting to do so;

- The resources used to produce an estimate could be better used on tackling fraud, for example, by carrying out more investigations.

These issues are dealt with below.

Producing reliable estimates

1.5 A number of departments have produced estimates of fraud or losses from fraud and error. For example, HM Revenue & Customs has produced estimates of overall losses on VAT and of particular types of loss such as missing trader fraud. This work is described in two documents – *Measuring Indirect Tax Losses 2007* and *Developing Methodologies for Measuring Direct Tax Losses* which are available on the HM Revenue & Customs website.

1.6 Departments have used operational research and statistical methods to produce such estimates. Two main methods used are *statistical modelling* and *sampling*.

Statistical modelling

1.7 Statistical modelling has been used to produce overall estimates of fraud or loss notably on revenue activities. This involves comparing levels of actual receipts or expenditure with the total level of receipts or expenditure that might be expected using other sources of data on the level of activity under review (**Figure 7**).

Figure 7

Examples of statistical modelling

Estimated evasion rates by the **BBC** on the television licence fee are calculated using a statistical model. In summary, the model estimates the level of evasion by subtracting the number of licences currently in force from the estimated number of properties for which a licence should be held. Repeating the modelling process at regular intervals has shown an overall downward trend in the evasion rate in recent years with the latest figures showing a rate of 5.1 per cent for 2006-07.

HM Revenue & Customs produce a top-down estimate for losses on VAT. This entails

comparing the total level of expenditure in the economy that is theoretically liable for VAT with actual VAT receipts and assuming that the difference represents the total revenue loss. The theoretical tax liability is a global measure based mainly on data from the Office for National Statistics. Bottom up estimates can be used in combination with the top level estimates as a means of validating the level of losses. Methods to produce bottom up estimates include surveys and use of administrative and operational data.

1.8 Points to consider for statistical modelling are:

- The data required may be incomplete. The model may use therefore a number of assumptions which mean that the results are subject to a margin of error. It is important to take this into account when making decisions on actions to reduce losses.
- Other work may be needed to give an insight into those committing the fraud or the type of action that might deter them. This may include more in depth modelling work (see Figure 12 on the BBC).
- Further research may be needed into the causes of increases or decreases in the level of losses and the extent to which this is due to anti-fraud measures implemented.

Sampling

1.9 Estimates of loss can be generated by checking a representative sample of cases to see whether fraud is involved, and extrapolating the results to the whole population to estimate the total level of fraud loss in the area of expenditure or revenue (**Figure 8**). When checking individual cases it can be difficult to determine whether any discrepancy is due to fraud or error (recklessness, carelessness or ignorance) because of the judgements that need to be made. In its work in estimating fraud in individual expenditure streams, the NHS Counter Fraud Service is deciding whether fraud is involved by using the concept of fraud and burden of proof applicable in civil law – that is whether someone knowingly or recklessly obtained resources to which they were not entitled and the balance of probability. This is to ensure that all behaviour which can legally be determined as fraud is measured.

Figure 8

The Driver and Vehicle Licensing Agency use sampling to estimate the amount of evasion of Vehicle Excise Duty

The **Department for Transport** commissions a roadside survey of over one million passing vehicles annually in June to identify unlicensed vehicles. Statistical weightings are then applied to the observed evasion rate in traffic to calculate the estimated evasion in the overall stock of vehicles, and then the estimated Vehicle Excise Duty revenue loss. The results are used to report performance against targets for the Department and the Driver and Vehicle Licensing Agency.

1.10 A key consideration in producing an estimate of fraud loss on an area of expenditure/revenue is the level of accuracy required. A greater degree of precision produces more reliable estimates (essential for assessing any real change in the level of fraud over time) but at additional cost because the size of the sample required increases (**Figure 9**).

Figure 9

Generating precise estimates of fraud requires larger sample sizes and incurs higher measurement costs

The degree of precision of a fraud loss estimate depends on:

- the size of the sample checked. For example, the **NHS Counter Fraud Service** set sample sizes so that they can determine the level of fraud in each area to within to +/- one per cent;
- whether the sample is stratified according to the type of risk;
- use of skilled reviewers able to detect where fraud has occurred, the amount of loss suffered and the nature of the fraud;
- the quality control and validation arrangements to ensure the review process is correctly and consistently applied.

1.11 For some organisations, producing a national estimate may be sufficient. In others, it may be necessary to produce estimates which are also broken down by region. This will have important implications for the sampling exercise and its costs, as separate samples within each region increase the total sample that must be checked (**Figure 10**).

Figure 10

Generating regional estimates of fraud loss involves larger sample sizes

Where a department needs estimates of the fraud loss within each of its regions, it will have to take a separate sample of transactions in each. To produce estimates that are sufficiently precise to reveal any important differences between regions in the rate of fraud loss requires the sampling of a much greater total number of transactions than when generating only a national level estimate.

Regional sampling will reveal which regions suffer the greatest and lowest levels of fraud loss and whether there are significant changes between regions over time.

The Department for Work and Pensions' random sample of over 40,000 cases a year covered each of nearly 100 districts, three times a year, split between each type of benefit claimant.

Costs of estimating fraud

1.12 As indicated above, the costs of measurement vary according to:

- the frequency of the estimating exercise;
- the sample sizes checked;
- the work involved in checking each case sampled;
- the work involved in validating the results.

1.13 For smaller departments and agencies, a one-off estimate or one produced at intervals may be sufficient. Accepting less precision by using smaller sample sizes may be one way forward. Although the results will be less reliable, these will indicate whether further work is desirable. Others may require continuous measurement exercises to produce ongoing estimates of fraud loss. While this involves greatest cost, it does mean that a department is able to track changes over time in the estimated fraud loss, and the types of fraud committed. **Figure 11** outlines the Department for Work and Pensions' continuous measurement approach.



Figure 11

The Department for Work and Pensions' continuous measurement approach

The **Department for Work and Pensions** spent over £9 million in 2006-07 as part of their ongoing measurement of fraud and error in Income Support, Jobseeker's Allowance, Pension Credit and Housing Benefit. The latest estimate shows that for the period October 2006 to September 2007, fraud losses were £210 million on Income Support, £60 million on Jobseeker's Allowance, £110 million on Pension Credit and £140 million on Housing Benefit. Total losses across all benefits were around £800 million or 0.6 of expenditure.

The Department produces estimates of the incidence and magnitude of fraud, customer and official error in these benefits every six months.

The Department has carried out a programme of reviews for other benefits such as Disability Living Allowance produced in 2005 and Incapacity Benefit in 2001. The Department's aim is to produce snapshot estimates of the amount fraud and error. The size and risk of potential loss determine which benefits are reviewed and how frequently.

1.14 Costs can be spread over several years by carrying out a rolling programme of estimates. For example, the NHS Counter Fraud Service has set out to measure fraud across the Primary care services including the pharmaceutical, optical and dental services. Three exercises have been carried out across each of these areas. Exercises are also underway looking at fraud within the procurement process. Another alternative is to carry out a one-off measurement exercise (with possible follow up several years later) to confirm the significance of the level of fraud. This can be a useful approach where the level of fraud is thought to be less significant.

Understanding the types of fraud risks

1.15 A department or agency will be unable to develop an appropriate response based only on the estimates of fraud. They also ideally need to know:

- the types of fraud perpetrated against them, for how long and the financial loss involved;
- who the fraudsters are, their characteristics and behaviours, how often they carry out the frauds, which types of frauds they commit, how they do it, and whether they are opportunistic or organised.

1.16 Examination of detected fraud cases either from investigation or from the random samples of cases examined to produce estimates of fraud loss, can give an insight into these (Figure 12). Larger departments which face serious threats also have intelligence analysts and/or commission research into the threats. At the other end of the spectrum, there are some departments and agencies that may have few or no recent instances of external fraud. Checking a sample of cases, or carrying out research into the possible threats, will help to confirm whether the risks from fraud are low.

Figure 12

Examples of work organisations have done to understand and manage fraud risks faced

The **BBC** has commissioned market research programmes, over a number of years, which have shown that evaders of the television licence fee vary both in their behaviour and their attitude to the licence fee. Overall the research indicates that non-payers are more likely to be younger people and less well off. They also tend to regard the licence as unfair or “just a tax you get nothing for”. Further research was carried out to model the evader population by matching evasion rates for postcode areas with commercially available data on income and life style. This information helped to identify the characteristics of those most likely to evade. Areas with high evasion rates are most likely to have, for example, a higher than average proportion of younger people, low income households, students and single parent families.

The **Department for Work and Pensions** collects information about the types of fraud, the characteristics of the customers and the way the fraud and customer errors are detected. These help the Department target resources to detect and prevent fraud.

For example, the Department estimates that the most common benefit frauds in the period October 2006 to September 2007 were claiming as a single person, but living with a partner as husband and wife (£92 million); fraud committed by customers living abroad (£93 million) and undeclared earnings (£77 million). The Department recognises that these frauds are high risk, and it targets investigations at this type of fraud.

For Income Support, the Department generate separate estimates of fraud and error for each of their three main client groups – Lone Parents, Pensioners

and Disabled people/Others. The measurement reviews also provide estimates of the main causes of fraud and error and the proportion of benefits overpaid due to each cause. For example, this enabled the Department to estimate that in the period October 2006 to September 2007 the failure of lone parent claimants to disclose they were living together with a partner was the cause of nearly half of the amount overpaid for this reason across all benefits.

HM Revenue & Customs uses centralised risk assessment and analysis of bulk third party data to identify groups posing a high risk of understating taxable profits. It aims to develop campaigns to ‘leverage’ the effects of its anti-fraud work beyond the limited pool that can be directly investigated on a ‘one to one’ basis. The results show that its approach has reduced understated income.

Focusing resources on the most effective anti-fraud measures

1.17 There is no single package of measures which can be applied universally by departments and agencies to tackle fraud. Measures need to be tailored to the type and size of threat faced. In deciding which measures to use and the extent to which to use them some departments have assessed the savings that could be achieved by targeting their resources in a better way. Savings could arise in three ways:

- The direct effects from recovering amounts defrauded. Where the measures involve reallocating resources into existing activities the department can look at the current costs/savings as a basis for estimating the return from increasing the levels of counter fraud activity. Where new measures are proposed, it is good practice to pilot these beforehand to test and refine their operation, assess their likely effectiveness and the type of savings that can be achieved.
- The preventive effect, through improved future compliance from those previously detected committing fraud. For example, HM Revenue & Customs assumes that the VAT yield will increase immediately from businesses previously detected committing VAT fraud, but that this additional yield will gradually reduce if no further checks are subsequently made.
- The deterrent effects on others that become more compliant as they learn of the greater efforts being taken to crack down on fraud. In practice it can be very difficult to assess these deterrent effects with any accuracy and Departments do not always seek to do so.

Setting targets and monitoring performance

1.18 Some departments have set targets to stabilise or reduce fraud over a period of time (**Figure 13**). Focusing targets on the overall level of fraud or loss is a good way of assessing performance, and generally a better measure than the amount of fraud or loss detected. The latter is difficult to interpret if the full scale of fraud or loss is not known. Other measures of performance are useful complements to estimates of total fraud loss, such as changes in regional levels of loss, the cost of tackling fraud compared to the return obtained and the rate of recovery of detected frauds.

Figure 13

Examples of Departmental targets to reduce fraud and error

The Department for Work and Pensions

has a strategic objective to “pay our customers the right benefits at the right time”. Supporting this objective is the aim to “drive down levels of fraud and error to deliver a reduction in benefit expenditure overpaid to 1.8 per cent and underpaid to 0.7 per cent by 2011.”

HM Revenue & Customs has a strategic objective to improve the extent to which individuals and businesses pay the tax due and receive the credits and payments to which they are entitled.

Key outcomes are:

- increase tax and national insurance contributions actually received relative to the amounts that should be received;
- reduce the level of incorrect tax credit payments as a result of error and fraud as a percentage of finalised entitlement; and
- maintain take-up of entitlements to tax credits and child benefit.

1.19 Performance data on outcome targets may not be available until long after the period measured due to the amount of work involved in sampling cases, checking, calculation and validation of the results. To monitor performance in-year, managers may rely on output results to indicate whether the outcomes are likely to be achieved. For example, managers may monitor:

- the results of operational checks on transactions;
- fraud investigation activity and outcomes (see Part 3, **Figure 31**);
- number and types of sanctions imposed (see Part 3, paragraph 3.39 and **Figure 39**);
- rate of recovery of defrauded amounts detected (see Part 3, paragraphs 3.32-3.38).

Responsibilities for tackling fraud

1.20 The responsibility for tackling fraud and managing fraud risks start at the top of the organisation within the senior management board. At this level, ownership of fraud risks is assigned and responsibilities allocated for managing individual fraud risks. Although everybody in the organisation has a role to play in tackling fraud (paragraphs 2.5 to 2.7), some departments have also set up central units or focal points with responsibility for tackling external fraud. These have coordinated work on developing the department's strategies' ensuring their implementation, monitoring results and providing advice and guidance. Fraud can be a moving target as the scale and nature of the risks change, so that regular monitoring of the situation is needed to identify and respond to new threats. A focal point for tackling fraud can help. HM Revenue & Customs, Department for Work and Pensions and NHS Counter Fraud Service each have central units (**Figure 14**). Where fraud numbers and losses are significant, departments also have teams of professionally trained investigators or enforcement officers dedicated to investigating cases of fraud.

Figure 14

Examples on how departments have assigned responsibilities

The NHS Counter Fraud Service remit

"To have overall responsibility for all work to counter fraud and corruption within the Department of Health and the NHS with particular priority for countering fraud in Family Health Services."

The Department for Work and Pensions

The Fraud and Error Strategy Division is a central unit which advises on fraud policy. Cases sent for investigation are either referred to the Fraud Investigation Service or Customer Compliance, both of which sit within Jobcentre Plus.

- The Fraud Investigation Service investigates potential fraudulent attacks against all benefits made by the Department or administered on its behalf. It concentrates on those cases that are likely to result in a sanction.
- Customer Compliance was set up in April 2006 to deal with cases where a full criminal investigation is not deemed appropriate but where action is needed to: identify levels of incorrectness; put it right and recover any overpayment; and ensure future compliance. The approach involves a robust face to face interview with customers in receipt of benefit. The approach is intended to target investigation resources more efficiently on dealing effectively with the cases of fraud most likely to result in a criminal sanction.

1.21 Regardless of the arrangements in place, departments and agencies need to ensure that someone is fully responsible for ensuring that the plans for tackling fraud are implemented in the way intended and that sufficient resources are in place. That individual should also be responsible for performance against targets. There is no point in having a well thought out strategy if it is not then put into effect.



Revenue

Tax Return

for the year ended 5 April 2005

UTR
Tax reference
Employer reference

Date

Inland Revenue office address
Area Director

Your address

Telephone

Please read this page before you start to fill in your Tax Return.

For
Reference

TOSHIBA

CAPITAL

Revenue

Tax Return

ended 5 April 2005

Part 2

Detering and preventing external fraud

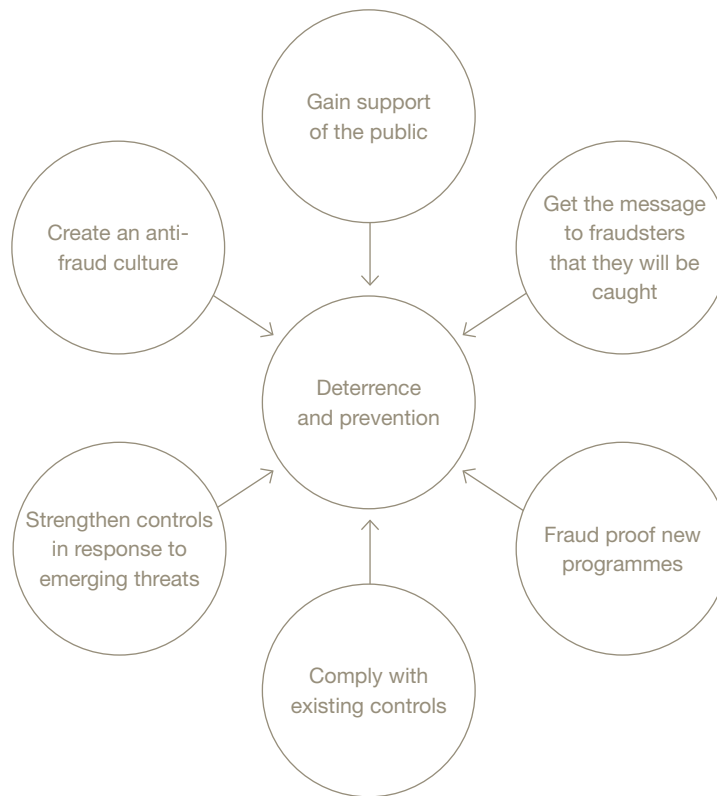
2.1 Deterrence involves convincing potential fraudsters that frauds against a department or agency are not worthwhile. Prevention measures aim to stop frauds entering departments' systems. Effective mechanisms for deterring and preventing fraud are essential elements in combating fraud. Realistically however, some fraudsters will never be deterred and not all frauds will be prevented. In these cases, prompt detection and professional investigations are needed (Part 3). Measures to deter and prevent fraud can be costly and departments need to ensure they are well designed for greatest effectiveness. **Figure 15** sets out the main elements for deterring and preventing fraud.

In looking at this Part of the guide ask yourself whether your organisation:

- seeks to influence customers' and the wider general public's attitudes to fraud;
- sends a strong message to potential fraudsters that they are likely to be caught and sanctions will be imposed. For example are there press releases on people/businesses prosecuted and are there any targeted or wider campaigns regionally or nationally?
- considers the fraud proofing of new programmes;
- ensures fraud controls are applied consistently and their use is monitored. What is the role of Internal Audit in this?
- considers strengthening controls where new fraud risks appear or where fraud starts to escalate;
- has an anti-fraud culture where staff understand the standards of conduct required and their personal responsibilities in preventing fraud; applying controls and reporting cases of suspected fraud.

Figure 15

The main elements for deterring and preventing fraud



Changing public attitudes to fraud

“National and local media campaigns continue to play an effective part of the Department’s strategy for tackling benefit fraud. As well as targeting hard hitting messages directly at actual and potential fraudsters, they also remind the public that benefit fraud is theft of honest taxpayer’s money. Combining clear messages that fraudsters will be caught and punished with continued awareness of the abuse of taxpayers’ money helps increase both deterrence and the social unacceptability of benefit fraud – two vital elements in maximising the fight against fraud.”

David Barr, Head of Fraud and Error Strategy Division, Department for Work and Pensions

2.2 Departments have sought to influence the attitude of customers and the wider general public to fraud by deterring those who might consider committing fraud and by making fraud socially unacceptable. The aim should be to get public support in the efforts to tackle fraud. Some deterrence messages Departments have used to deter potential fraudsters from attempting fraud are:

- strong controls will stop them from succeeding; followed by
- it is likely they will be caught;
- evidence of their fraud will then be discovered;
- they will thus face penalties; and
- amounts defrauded will be recovered.

2.3 Departments have used a variety of methods to publicise the success of their work, such as issuing press releases and putting information on their websites of cases prosecuted. These are cost effective actions which can be used by smaller departments and agencies. In the United States of America the Internal Revenue Service issues periodic “Tax Fraud Alerts” on their website warning the public of the risks and costs of buying into tax evasion schemes, as well as providing information on the latest “schemes, scams and cons”. The Alerts set out in more detail the main

strands of the Service’s enforcement programme and the consequences of non compliance. For example, for employment taxes, the relevant “Tax Fraud Alert” provides details of legal requirements, employer and employee responsibilities, examples of tax evasion schemes, and data on how non-compliance has been dealt with in the courts including specific significant examples. To strengthen their message, some departments have used media campaigns (**Figure 16**). Before introducing a national campaign, pilots can be used to test and improve the likely effectiveness.

Figure 16

Examples of Departmental campaigns to change public attitudes and to deter fraudsters

The approach used by the Department for Work and Pensions

The campaign has run in several phases, each with a different message and using different communication media. This aims to:

- reinforce honest behaviour by customers;
- create a climate of intolerance to benefit fraud among the wider public and undermine its social acceptability;
- deter potential fraudsters.

From September 2001, the campaign focused on dishonest claimants. Messages of deterrence and detection aimed to raise the fear of getting caught and portray the likely consequences. Scenarios used in television advertisements showed benefit fraudsters being caught or punished, or both. In addition, the campaign used radio and regional press advertisements, the latter featuring real newspaper headlines from fraud prosecutions.

In June 2003, the next phase used the slogan “We’re on to you”. It featured a spotlight that followed fraudsters in realistic scenarios, such as at work, to show them that they would be found out if they were continuing to claim benefits to which they were no longer entitled, and to warn potential cheats that benefit fraud is a serious crime.

In August 2003, a new phase used small posters on lampposts and in pub washrooms. Aiming to look like an offer of cash in hand work, the message stated that continuing to claim benefits while working was benefit fraud and would only earn the person a criminal record.

In November 2003, this phase was adapted. Small mock advertisements were placed in pubs, clubs and shop windows. The main message “Do you want to earn £££s and still sign on?” was designed to catch the eye of those considering cash in hand work, while continuing to claim benefits, to fund Christmas celebrations, and then to deter them from failing to report to the Department that they were now working.

In 2006, the Department started its “No ifs, no buts” phase of the campaign. This phase focuses on the benefit fraudster and targets their views that there may be excuses for committing benefit fraud which the campaign seeks to overturn. “No if, no buts” has been used in television and poster advertising, in local press and magazines, buses, and door drops, as well as on the Department’s website.

The Department arranges for independent evaluations of each phase of its campaigns. Research for the Department suggests that between 2005 and 2006 there was an increase from 75 per cent to 83 per cent of people who strongly agree that it is wrong to claim benefits to which they are not entitled.

The approach used by HM Revenue & Customs to encourage self-employed people to register for tax

HM Revenue & Customs ran a series of advertising campaigns at a cost of £2 million specifically to raise awareness amongst the self-employed to register for tax. It ran three advertising campaigns during the period June 2005 to March 2007. One of the main messages was “it is a simple process to register and we are there to help, ring our helpline”. The advertising campaigns focused on particular groups who may have failed to register for tax such as e-traders and landlords.

The initial campaign costing £1.5 million resulted in:

- An estimated additional 5,000 people calling the helpline to register. These are people who may have otherwise joined or remained in the hidden economy. HM Revenue & Customs estimates that it will collect £23 million in tax over three years from these people;
- A further 3,300 people called the helpline to request the “*Thinking of working for yourself?*” and if these people register HM Revenue & Customs would collect an estimated £15 million in tax over three years.

2.4 To maximise the deterrent effect, departments have:

- researched fraudster behaviour and risk taking/aversion to determine which messages will be most effective in changing their behaviour;
- designed media messages to achieve maximum effect;
- used relevant media to ensure potential fraudsters are aware of these messages;
- refreshed messages regularly to maintain a strong deterrent effect;
- developed performance indicators to evaluate the effectiveness of the approach. It can however be difficult to make a direct link between the campaign and reductions in fraud levels, because of other anti-fraud measures also in force;
- fed back the evaluation into renewed campaigns to deter fraudsters.

Changing staff attitudes to create an anti-fraud culture

“Creating an anti-fraud culture involves having a clear statement of ethical values, promoting staff awareness, recruiting honest staff and maintaining good staff morale”

Managing the Risk of Fraud: A Guide for Managers, HM Treasury

2.5 Creating an anti-fraud culture, in which all staff understand the standards of conduct required, their personal responsibilities in preventing fraud and the importance of controls, is vital in preventing external fraud, as **Figure 17** illustrates. Publicising internally the organisation’s strategic approach to tackling fraud and what it is trying to achieve can be a good way of reinforcing the anti-fraud culture.



Figure 17

The NHS Counter Fraud Service have emphasised the value of an anti-fraud culture in preventing fraud

The creation of an anti-fraud culture is one of the primary aims of the **NHS Counter Fraud Service**. Local Counter Fraud Specialists, who are employed by health bodies, are also responsible for creating an anti-fraud culture and are well placed to target those areas within their health bodies where fraud awareness may still be low.

The NHS Counter Fraud Service has implemented a number of initiatives to raise awareness of the issue and the role that NHS staff can play in preventing and deterring fraud, including:

- delivering fraud awareness presentations to key audiences both within the NHS and to external agencies;
- developing close working relationships with stakeholders across the NHS and signing counter fraud agreements with regulatory and professional bodies representing over 1.4 million NHS staff and professionals;
- publishing the quarterly magazine *Insight* which spreads good practice and seeks to strengthen further the anti-fraud culture;
- obtaining media coverage in newspaper articles, radio broadcasts and television programmes. These can play an important role in raising fraud awareness and deterring those who may commit or seek to commit fraud;
- running awareness campaigns such as Fraud Awareness Month to promote the role of the Local Counter Fraud Specialist, informing staff how they can report suspicions of fraud and generate referrals;
- providing Local Counter Fraud Specialists with resources to assist them in raising awareness on a local level and in promoting the Fraud and Corruption reporting line – 0800 028 40 60.



2.6 Training can help raise staff awareness of the risks of external fraud and the importance of compliance with internal control procedures and security checks to prevent such frauds. And close monitoring of staff compliance with these controls helps ensure their consistent application. Training may take several forms such as:

- fraud awareness workshops for a wide range of staff;
- targeted personal mentoring for staff working in areas found to be vulnerable to fraud;
- closer managerial supervision with feedback to staff on their compliance with security procedures.

2.7 A staff survey or focus group may be used to test staff attitudes to security, and their compliance with controls to prevent fraud. The findings from such research can help identify opportunities to improve prevention and to strengthen internal controls, identify any messages that need to be reinforced, reveal any areas where compliance with prevention controls is insufficient and generate further information about the frauds identified by staff.

Controls to prevent fraud

“It is always possible to have controls which prevent fraud, but such controls need also to enable Departments to give a timely service to honest customers, without unacceptable burdens. Designing effective controls depends on understanding the scale and nature of the risks and the costs.”

Caroline Mawhood, Assistant Auditor General,
National Audit Office

2.8 There are a range of controls (for example, physical checks, reconciliation, supervisory checks and clear roles and responsibilities) that address risk, including fraud. Departments and agencies need to consider which controls are most appropriate in their particular circumstances. The consistent application of internal controls can be highly effective in preventing fraud losses. Internal Audit should provide assurance on the operation of those controls and their effectiveness in preventing fraud. Internal controls can impose both internal and external costs from their operation. Controls need to be designed which are proportionate to the risk, while enabling the organisation to deliver the services to its customers to meet their needs.

2.9 Two key aspects to prevention are:

- “fraud-proofing” new programmes and systems;
- consistent application of existing controls and strengthening of these where needed.

Fraud proofing new programmes and systems

2.10 Organisations need to recognise their responsibility when designing and implementing new policies, programmes and systems to build good controls in to manage fraud where there are vulnerabilities or to fraud proof them by designing them to be inherently less vulnerable to fraud. Complex rules of entitlement can increase the risks of fraud. Fraudsters can exploit the situation in two ways. The rules may be difficult to police effectively, requiring officials to consult volumes of guidance in their everyday work. Where customers are often uncertain of their obligations, it is easier for fraudsters to misrepresent their circumstances and if discovered claim that it was a genuine error.

2.11 Sufficient weight should be given to expert advice on the risks of fraud in new programmes and effective counter fraud measures should be integrated into the design. Where innovative schemes are being proposed, it is good practice to pilot these to identify any further risks of external fraud. Early consultation with internal audit and counter fraud specialists can help to identify the risks, and to obtain advice on how these can be minimised, at key stages during design and implementation of new programmes. An evaluation process is helpful in determining whether early risk assessments have been effective in countering fraud risks during development, piloting and initial implementation.

2.12 The NHS Counter Fraud Service liaises with policy leads across the Department of Health and Government in an ongoing initiative to fraud proof the Department’s future policies. The aim is to ensure that, as far as possible, new and existing NHS schemes are protected from fraud from the outset. **Figure 18** shows steps taken to fraud proof the Department of Health’s Healthy Start scheme. The scheme offers free milk, fruit and vegetables to mothers on eligible benefits and beneficiaries are sent vouchers to exchange for these goods at approved retailers. Retailers then send the vouchers to the Department of Health for reimbursement.

Figure 18

The steps taken to ‘fraud proof’ the Healthy Start Scheme

Clear Rules

- Analysis of the Healthy Start regulations to identify fraud risks.
- Introduction of application forms for beneficiaries and retailers to join the scheme.
- Strict terms and conditions with counter fraud information placed on all literature.

Prevention

- Physical security methods placed on the Healthy Start voucher – anti-photocopying paper, watermarks.

Accountability

- Unique information included on the Healthy Start voucher – National Insurance Number, unique barcodes and sequential numbering.

- Appropriate declarations placed on forms to warn of the consequences of committing fraud.

Monitoring

- Detection methods for Department of Health subcontracted administrators – a new payment machine that scans vouchers sent by retailers for reimbursement which identifies copied vouchers and prevents duplicate payments.
- Warning letters automatically sent to beneficiary and retailer if attempt at duplicate payment occurs.

Sanctions

- Removal of retailers from the scheme if convicted of fraud (in conjunction with a court ruling).

Strengthening internal controls and checks

2.13 It is important that the effectiveness of controls is continually reviewed. Controls which have traditionally worked well in countering fraud may no longer be effective where fraudsters have launched determined attacks. Detected cases of fraud may show that fraudsters are using new methods to circumvent controls indicating that these need to be strengthened. Internal Audit's work may also identify system weaknesses which could lead to fraud.

2.14 In 2003, the NHS Counter Fraud Service set up a Fraud Prevention Unit to identify specific areas of weakness in systems, recommend policy changes where appropriate and issue instructions and guidance to make them less vulnerable to fraud (**Figure 19**). A recent fraud prevention review involved the Unit examining the processes within trusts for identifying chargeable overseas visitors. The findings and recommendations from the fraud prevention review have been provided to the Department of Health to help with developing further regulations and guidance. The latest fraud prevention instruction issued by the Unit arose from an investigation into an allegation of fraud that a Primary Care Trust was being falsely invoiced for services. The investigation led to the introduction of standard claim forms, which include counter fraud declarations.

Figure 19
The methodology used by the NHS Counter Fraud Service Fraud Prevention Unit

Action by the Fraud Prevention Team

- 1** Identify possible areas of high risk of fraud in the NHS arising from system weaknesses. Sources will include the staff within the Counter Fraud Service including the Central Intelligence Unit, Risk Measurement Team, Quality Team and feedback from Local Counter Fraud Specialists.
 - 2** Research the areas of system weakness and establish the amounts at risk.
 - 3** Organise a programme of visits to selected NHS Trusts to gain experience of how the systems work in practice.
 - 4** Issue questionnaires to NHS Trusts to assist in identifying the scale of any system weaknesses.
 - 5** Collate the findings and recommendations from the research, reviews and questionnaires.
 - 6** Issue instructions, best practice guidance and/or recommend policy change taking into account the amounts at risk.
 - 7** Request compliance statements from NHS Trusts to provide assurance that good practice is being applied.
 - 8** If appropriate, recommend that Local Counter Fraud Specialists carry out proactive fraud prevention work into the areas of high risk identified.
 - 9** Measure the financial impact of the introduction of any new procedures.
 - 10** Report findings, recommendations and action taken to Counter Fraud and Security Management Service policy, operational, and intelligence services as appropriate.
-

2.15 Strengthening internal controls can also help prevent or reduce criminal attacks. For example, the most serious VAT fraud that HM Revenue & Customs currently face is VAT missing trader fraud – a Europe-wide systematic attack on the VAT system orchestrated by organised crime groups. As part of its strategy, introduced in September 2000, to tackle this fraud, HM Revenue & Customs enhanced their VAT registration checking procedures to make it easier for it to detect and prevent bogus registrations. Each VAT application form is assessed according to various risk criteria to identify potential fraudsters. Further checks are carried out on suspect applications and those that remain suspect are visited. The number of suspect registration applications refused increased from around 3,500 in 2005-06 to around 6,000 in 2006-07.

2.16 New legislation may be required to improve controls. **Figure 20** illustrates how improved legislation has helped to reduce fraud in HM Revenue & Customs.

Figure 20

Shows how HM Revenue and Customs has improved fraud controls by introducing new legislation

Missing Trader Intra-Community fraud is a systematic criminal attack on the VAT system that is recognised as a serious problem throughout the European Union. The Government's strategy for tackling it was strengthened in response to a rapid and large rise in attempted fraud in 2005-06. This targets the people, goods and money flows associated with the fraud using measures including:

- legislation to make traders jointly and severally liable for VAT debts and to change the VAT accounting practice on domestic business-to-business supplies (a 'reverse charge') for the most commonly traded goods which involve missing trade fraud;
- operational activity, including rigorous checks on suspect applications for VAT registration, and the use of dedicated teams to carry out in-depth verification of suspect VAT repayment claims; and
- criminal investigation and prosecution of those involved in the fraud, and the recovery of the proceeds of their crimes.

As a result of the strategy, HM Revenue & Customs estimate that attempted fraud has fallen by up to £1.5 billion in 2006-07, to between £2.25 billion and £3.25 billion.

2.17 Developments in technology can provide opportunities to strengthen controls in a cost effective manner to reduce the level of external fraud. **Figure 21** illustrates how new technologies are used to prevent fraud.

Figure 21

Examples of how new technology is being used to prevent and detect fraud in the private sector

The Association for Payment Clearing Services (APACS) has reported that the success of chip and PIN has meant that face-to-face credit card fraud has continued to drop, falling, in 2006, a further 47 per cent on 2005 levels. The chip cards prevent counterfeiting of cards by holding data securely preventing copying or alteration. The use of a four digit number PIN number also helps reduce the use of stolen cards.

The insurance industry uses Voice Risk Analysis to speed up the processing of claims and to identify possible higher risk claims. The technology detects minute changes in a caller's voice caused by stress levels which give signs as to when the caller may be lying about their circumstances. It then assigns a risk profile to that caller. This prompts the call handler to probe more deeply into the information provided by the caller. There has been some criticism about the use of voice risk analysis for the purpose of tackling fraud with it being described as a lie detector that could deter genuine customers from claiming benefits.

The Department for Work and Pensions is trialling the technology within 7 local authority sites on Housing Benefit and Council Tax Benefit claims and a Jobcentre Plus call-centre. Expenditure on Voice Risk Analysis by the Department in 2007-08 was £700,000 of which £460,000 was paid directly to local authorities piloting the technology. In May 2008 a further £1.5 million was made available for 15 local authorities' trials. The Department will evaluate the technology in August 2008 and has commissioned social research into the customer experience and whether or not it deters genuine customers from claiming benefits. Following this evaluation, the Department will assess whether the technology should be tested more widely.

Part 3

Detecting and investigating external fraud and imposing sanctions

3.1 To show that departments and agencies are serious about tackling external fraud, they need to detect cases of fraud against them; investigate them where appropriate and impose sanctions which are proportionate to the crime. This will help to deter potential fraudsters in the future by showing that crime does not pay, especially if the outcomes of cases are well publicised. Departments also need to consider whether the frauds detected show new threats are emerging, or are on a larger scale than originally thought. From this work, departments and agencies will need to consider whether their strategic approach needs updating. They will also need to assess whether any frauds reveal systemic weaknesses which need to be tackled (**Figure 22**).

In looking at this Part of the guide, ask yourself whether your organisation:

- has a well publicised telephone hotline, email and freepost address to which the public can report cases of suspected fraud;
- uses techniques proactively to detect cases of suspected fraud such as in-depth investigative work into “hotspot” areas, data matching exercises, data mining and neural networks as appropriate;
- assesses whether suspect cases of fraud need to be investigated further such as through the use of scoring systems;
- assesses whether the number of investigations is proportionate to the potential sums lost from fraud;
- tracks the progress of individual investigations;
- has sufficient investigative staff with the essential technical knowledge and experience;
- reviews independently the way fraud investigations have been conducted;
- imposes appropriate sanctions on fraudsters such as fines, or other penalties, or refers appropriate cases for criminal prosecution;
- seeks to recover the amounts lost from fraud;
- evaluates the effectiveness of sanctions;
- works with others to tackle fraud.

Figure 22

The actions to deal with individual cases of fraud



Detecting fraud

“Effective work to detect and investigate fraud must lie at the heart of any professional, integrated approach. Such work is not only about eventually applying appropriate sanctions, it has to be about learning as much as possible about the nature of the problem, about deterring fraud where this is possible and about identifying the policy or systems weakness which has allowed it to occur.”

Dermid McCausland, Managing Director, NHS Counter Fraud Service

3.2 Frauds may be detected in a number of different ways. Referrals may come from staff who have carried out checks on transactions and suspect a fraud. Members of the public may contact departments about their suspicions. Departments may also use a range of techniques and technologies to identify suspicious cases for further investigation. They may also carry out special pro-active exercises to detect fraud in high risk areas. Fraud investigators may develop their own intelligence by following leads on existing cases where there may be links to other frauds.

This section focuses on the use of hotlines and computer software techniques.

Hotlines

3.3 Hotlines can be a cost effective way of obtaining from staff and the public details of possible cases of external fraud which can be assessed and investigated further. **Figure 23** outlines the arrangements in place in some departments. Good practices include:

- setting up a single freephone telephone number, with alternative means of contacting the department including an email and freepost addresses;
- advertising the telephone number and contact details on the department's website, in leaflets and posters, advertisements during anti fraud campaigns;
- giving undertakings on confidentiality; indicating the information that is useful in a referral, including the types of frauds that the department are particularly interested in hearing of and how the department will deal with the information provided.

3.4 It is also good practice to record information received onto a standard form. This can help in prompting the person making the referral into providing as much relevant information as possible. An electronic version of the form can be included on a website, which can be completed and submitted anonymously online. The person may want to know what action may be taken and feedback on what has happened. While it is possible to give general information on how referrals are handled, it may well not be possible to give specific details on individual referrals where this would breach confidentiality requirements.

3.5 Hotlines should be evaluated at regular intervals, for example, analysing the number and type of referrals received, what has happened in each case, and overall results.

Figure 23

How some departments are using hotlines

The Department for Work and Pensions has a dedicated telephone hotline (0800 854440) and website (www.dwp.gov.uk/benefit-thieves) to support the public in reporting suspicions of benefit fraud. In 2007-08, the hotline received 250,000 calls from the public.

The **NHS Counter Fraud Service** has a confidential NHS Fraud and Corruption Reporting Line (**0800 02840 60**) which NHS staff and the public can ring to report suspicions of fraud.

Members of the public can anonymously report a vehicle that appears to be unlicensed and used/kept on the public highway to **The Driver and Vehicle Licensing Agency** by using the national untaxed vehicles telephone hotline on freephone (0800 0325202), by completing an online form or by writing to a DVLA local office. The Agency receives around 10,000 reports a month from the public.

In November 2005, **HM Revenue & Customs** set up a confidential Tax Evasion Hotline (0800 788 887) allowing members of the public to report suspicions on the evasion of income tax, corporation tax, capital gains tax, inheritance tax, VAT or National Insurance contributions. The hotline takes calls Monday to Friday 8am to 8pm, Saturday and Sunday 8am to 4pm. People can also report details of their suspicions through the Department's website by completing an online form. In March 2006 the Department commissioned a major advertising campaign, using a combination of TV, press and radio to encourage members of the public to use the hotline. The hotline received around 120,000 calls in 2006-07. The number of calls has averaged 7,000 a month since then.

The use of computer techniques to detect fraud

3.6 A range of techniques using computer software and technologies can be used to detect cases of fraud. These include techniques such as data matching, data mining and neural networks. Smaller departments and agencies may be able to draw on the experience and lessons of others in the use of these techniques.

3.7 *Data matching* involves computerised scanning of data held in different data files either within the same organisation or in different organisations. It can be used by management for a range of purposes including detecting potential fraud. With increasing computer power, data matching across files is possible on a very large scale.

3.8 To help focus resources on the matches which indicate possible fraud, data matching software:

- highlights the highest priority matches;
- allows users to filter only those matches that meet investigators' criteria for investigation;
- explains the importance of each match type and protocols for sharing information between matched bodies.

3.9 The Audit Commission's National Fraud Initiative is the country's largest data matching exercise in relation to fraud (**Figure 24**). The National Fraud Initiative will be expanded in future years as a result of a new statutory power under Part 2A to the *Audit Commission Act 1998* as amended by the *Serious Crime Act 2007*.¹⁰ The Act enables bodies other than those that have a mandatory requirement to provide data for the National Fraud Initiative to volunteer to participate by providing data to the Commission. This means that central government departments and agencies can participate in future data matching exercises. **Figure 25 to 27** shows how the Department for Work and Pensions, the Driver and Vehicle Licensing Agency and HM Revenue & Customs use data matching to detect evasion.

¹⁰ *Serious Crime Act 2007* – http://www.opsi.gov.uk/ACTS/acts2007/ukpga_20070027_en_1

Figure 24

The Audit Commission's National Fraud Initiative

The **National Fraud Initiative** is the country's largest public sector anti-fraud exercise. It is a computer based system which is run every two years and matches information such as housing benefit claims, pensions and social housing records from local councils, the NHS, police authorities, local probation boards and fire and rescue authorities across England.

The matching process enables public bodies to share and compare information through a secure website and identify those taking services or money that they are not entitled to. Typical examples include council tenants renting (and sub-letting) council property in two different authorities, fraudulent claims for housing benefit, pensions being claimed for deceased people, fraudulent use of blue badge parking passes and duplicate trade creditor payments.

A record £140 million in fraud and overpayment was detected by the National Fraud Initiative in 2006-07. The National Fraud Initiative has now detected around £450 million in fraud and overpayments since it started in 1996.

Figure 25

Shows how the Department for Work and Pensions is using data matching

The **Department for Work and Pensions** has a dedicated Database and Matching Service to identify possible fraud and error. It matches data:

- across benefit systems;
- between other Government departments and Department for Work and Pensions data;
- for other Government departments;
- for Local Authorities on Housing and Council Tax Benefits;
- to tackle internal fraud.

The Department for Work and Pensions is currently modernising its Database and Matching Service to deliver a more timely and streamlined service to its customers. The objectives are to:

- modernise the extraction of data from data systems to provide electronic transfer, cutting down on clerical and manual interventions;
- operate a fraud and error referral system from a modern IT platform which allows new risk analysis techniques to be used;

- provide an integrated service centred around the customer rather than the product;
- provide more frequent and timely referrals.

The programme aims to provide regular and timelier feeds into the data matching system to prevent frauds from being in the system for long periods of time. Fraudsters are therefore more likely to be caught sooner, and overpayments are expected to reduce as a result.

Figure 26

Shows how the Driver and Vehicle Licensing Agency uses data matching to detect vehicle excise duty evasion

Automatic Number Plate Recognition (ANPR) cameras, some fixed and some mounted in mobile units, collect images of stationary and moving vehicles. Computer software searches for images of number plates and records the registration mark. The recorded mark is then compared with details from the Agency's vehicle database. If a match is found, the image and event details are stored as evidence of the offence. The images of vehicle registration marks that are not matched to the unlicensed vehicle data bank are discarded.

Figure 27

Example of how HM Revenue & Customs has used data matching

Using data matching, **HM Revenue & Customs** has identified people who may have received income from property but have not disclosed it. Following on from an advertising campaign, HM Revenue & Customs is sending letters to taxpayers for whom it holds information suggesting that they may have received income from letting property. The letters contain clear guidance, along with a standard form that can be used to return details of income received. Where no reply is received, HM Revenue & Customs considers what further action needs to be taken which could include formal enquiry or, in exceptional cases, criminal investigation.



3.10 The *Serious Crime Act 2007* enables a public authority to disclose information as a member of a specified anti-fraud organisation for the purposes of preventing fraud or a particular kind of fraud. The information may be of any kind and may be disclosed to the specified anti-fraud organisation, any members of it or any other person to whom disclosure is permitted. As part of the regulatory impact assessment for the new provision, four public sector organisations provided in total 1,636 records to match against CIFAS' database. CIFAS is a Fraud Prevention Service with 270 member organisations spread across banking, credit cards, asset finance, retail credit mail order, insurance and other sectors. Nearly one third of the records matched demonstrating that many of those who commit fraud against one organisation also commit fraud against others.

3.11 Data matching between different bodies is facilitated greatly by common data descriptors but is possible only if there is appropriate authority for data to be transferred or shared between these bodies. This authority may derive from a statutory basis for demanding, or disclosing, the data or both. Uncertainty regarding powers to share data may sometimes have hindered the use of data matching. Data matching has also raised concerns about the possible infringement of individual rights to privacy. Concerns about individual privacy are the subject of the *Data Protection Act* and the *Human Rights Act 1998*.

3.12 The Information Commissioner has issued guidance on his website listing the eight principles put in place by the *Data Protection Act 1998* which ensure that information is handled properly. These are that data must be:

- fairly and lawfully processed;
- processed for limited purposes;
- adequate, relevant and not excessive;
- accurate;
- not kept for longer than is necessary;
- processed in line with the individual's rights;
- secure;
- not transferred to countries without adequate protection.¹¹

The Commissioner has also produced guidance on implementing these principles in the documents on Compliance advice: Data sharing between different local authority departments; Framework code of practice for sharing personal information; Sharing personal information in the public sector: A new approach and Sharing personal information: Our approach.

3.13 Schedule 8 of the *Human Rights Act 1998* gives rise to questions about the extent to which data matching complies with the provisions regarding personal rights to privacy. There are exceptions to these provisions where:

“necessary in a democratic society in the interests of national security, public safety or the economic well being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others”¹²

¹¹ *Eight principles of the Data Protection Act 1998*, Information Commissioner's Office
http://www.ico.gov.uk/what_we_cover/data_protection/the_basics.aspx

¹² *Human Rights Act 1998 Chapter 42* – <http://www.hmsa.gov.uk/acts/acts1998/19980042.htm>

3.14 Data mining is the process of selecting, exploring and modelling large amounts of data to reveal previously unknown patterns, behaviours, trends or relationships which may help to identify cases of fraud. Because of the large amount of data that need to be analysed, specialist computer software is used which usually contain a range of data mining tools (**Figure 28**). A number of software companies have developed such products. Data mining can be a powerful way of interrogating data and revealing anomalies that would not be revealed by other techniques. However, to enable it to function most effectively, staff need to be trained in the use of the software, and to gain experience in selecting the most appropriate tools to scrutinize the data and in following up anomalies to detect cases of fraud.

Figure 28

How some organisations have used data mining

The **BBC** uses data mining software tools to match details of licensable places with external commercially-available data to identify specific places or segments of the population for targeted enforcement activity. The facility has been used to target mailshots, posters and telephone chasing on specific groups, such as students, and offers opportunities to focus enforcement activity on places or segments of the population where the likelihood of evasion is greatest.

The **NHS Counter Fraud Service** uses data mining and analysis software to examine pharmaceutical and dental data. The software is capable of advanced data analysis that establishes data profiles and highlights anomalies. These can indicate potential fraud for further investigation. For example, the software highlights any individual dentist claiming for unusually high levels of intricate or expensive work. These cases are identified for potential investigation of whether the dentist is making fraudulent claims.

3.15 Neural networks are computer based multiprocessing systems which are designed to connect data from multiple sources to identify structures and patterns and exceptions to an identified structure or pattern. The ability of neural networks to identify patterns of activity and exceptions to a pattern that may be associated with fraud, gives organisations an ability to focus their detective efforts on these exceptions.

3.16 One of the problems of using these techniques more widely in the public sector is that the data may not be held in a way that lends itself to such analysis. The move towards providing services online may change this and allow real time analysis of transactions through Departments' websites using some of these techniques.

Investigating cases of fraud

3.17 Where fraud has occurred, the Department should consider:

- stopping the fraud at the earliest opportunity and look at whether weak controls have been exploited which need to be tightened up;
- whether to refer the case for criminal prosecution or impose a penalty;
- collecting any arrears and any penalties to ensure that the economics of the crime are undermined and to deter others.

3.18 Some departments have criteria or scoring systems to determine those that should be investigated with a view to prosecution with the remainder subject to other forms of sanction. An intelligence and risk based approach to assigning cases for investigation is used by the Department for Work and Pensions (**Figure 29**) and HM Revenue & Customs has set out criteria for cases submitted for criminal investigation when serious frauds are suspected (**Figure 30**). Unlike the larger Departments, smaller departments and agencies may not have trained fraud investigators in which case they will need to involve the Police in dealing with detected cases of external fraud. They also need to have plans in place so that they know the steps to take if cases are uncovered.

3.19 Departments also need to look at whether the total number of investigations is commensurate with the potential sums lost from fraud. The costs of investigating cases can be resource intensive. Assessing the financial return achieved on the overall caseload, and different categories of case will indicate the likely benefits of undertaking more investigations or a different mix.

Figure 29

The Department for Work and Pensions has a dedicated intelligence function to evaluate cases of potential fraud and decide which to investigate

| | |
|--|--|
| The Department for Work and Pensions has a network of 10 Operational Intelligence Units located across England, Scotland and Wales. When referrals are received for investigation the Fraud Referral and Intervention Management System (FRAIMS) applies a rules engine that determines routes for investigation and provides a Gateway through which cases can be channelled. | This clarifies whether cases should be investigated via the Fraud Investigation Service or Customer Compliance route (see Figure 14). For fraud investigation cases, the Operational Intelligence Units then gather and evaluate intelligence on cases to assist fraud investigators, including exchanging information with other agencies where appropriate. |
|--|--|

Figure 30

HM Revenue & Customs uses criteria for deciding which cases to refer for criminal investigation

HM Revenue & Customs has a published policy setting out the types of behaviour it will usually consider for criminal investigation. These include factors such as whether the fraud is an attack on the system, the type of person carrying out the fraud and previous behaviour. The objective of the criteria is to ensure that resources can be targeted where they have the greatest effect on compliance. Whenever a case is referred for possible criminal investigation HM Revenue & Customs evaluate it against these criteria, as well as considering the strength of available evidence and likelihood of a successful investigation.

3.20 Tracking the progress of fraud investigations allows managers to assess the overall workload (such as whether investigations are concentrated on the main types of fraud set out in the Department’s strategy); identify problem areas such as where progress is slower than would be expected; understand the cost implications of investigations and the effects on planning future resource usage or the consequences of increasing or decreasing resource levels (**Figure 31**).

Figure 31

Information to help managers track fraud investigations

- Useful information can include:
- number of investigations carried out;
 - value of fraud loss identified;
 - duration of individual investigations;
 - costs of individual investigations;
 - methods of investigations used;
 - outcome of investigations (prosecutions; fines etc).

3.21 Where departments investigate frauds they will need to consider whether there are sufficient staff with the right technical and investigative knowledge and experience. The Counter Fraud Professional Accreditation Board was set up in 2001 as a professional body for counter fraud specialists. It sets professional conduct guidelines for its members who have successfully completed the specialist counter fraud training and university courses. **Figure 32** sets out the development of a professional and ethical approach to countering fraud by the NHS Counter Fraud Service.

Figure 32**The NHS Counter Fraud Service approach to counter fraud work**

In 1999 the NHS Counter Fraud and Security Management Service devised a professionalism strategy, which set out the competencies required for counter fraud specialists and established a series of practical skills-based training courses that collectively formed a Foundation Level. It is mandatory for everyone in the NHS who counters fraud to receive this training and by 2008 over 800 people in the NHS have successfully completed it.

The Department for Work and Pensions, HM Revenue and Customs, local authorities, Identity and Passport Service, the Border and Immigration Service, Child Support Agency, Abbey National and Capita Ltd. Have all adopted the Foundation Level and the qualification of Accredited Counter Fraud Specialist. By 2008, over 10,000 held the qualification.

The Foundation Level has been accredited by a number of universities specialising in criminal justice. The *Certificate of Higher Education in Counter Fraud and Criminal Justice Studies* (Advanced Level) is the first academic qualification specifically for the counter fraud field and hundreds of students have proceeded from the Foundation Level to study for the Advanced Level. There is also a BSc. (Hons) in Counter Fraud and Criminal Justice Studies.

Since 2007 there is an NHS-developed *MSc Counter Fraud and Corruption Studies* specifically designed to meet the needs of graduates and professionals specialising in countering fraud and corruption. It seeks to equip students with a critical knowledge base following the introduction of the *Fraud Act 2006*, the Government's Fraud Review and the changes in corruption legislation.

3.22 Other large departments provide a range of training for fraud investigators. For example, HM Revenue & Customs has developed procedures, provided training on these for all investigators and implemented an assurance process to ensure that investigators adhere to them. New investigation recruits are given 14 weeks of training in basic investigation techniques which can be followed by more specialist courses such as the handling of informants. The investigators are also supported in their work by specialists such as forensic accountants and computer analysts.

3.23 In the Department for Work and Pensions, a programme of training is provided for investigative and intelligence officers and managers as well as those from local authorities. Investigators in the Fraud Investigation Service receive Professionalism in Security (PINS) training which is accredited by Portsmouth University. Additional guidance is provided in the Fraud Procedures and Instructions Manual which is regularly updated.

3.24 Investigations into fraud should be consistent with the aims of the criminal justice system to reduce crime and the fear of crime and to dispense justice fairly and efficiently, promoting confidence in the rule of law.¹³ Fraud investigations need to be of high quality. Independently reviewing the way in which fraud investigations have been carried out can help to ensure that appropriate standards and legal requirements have been followed. The findings can highlight areas where improvement is needed. The reviews can be undertaken by:

- independent internal teams, with expertise in fraud investigation, to review the conduct and quality of fraud investigations;
- Surveillance Commissioner (<http://www.surveillancecommissioners.gov.uk/>) for use of covert investigative methods;
- the appointment of an external assessor.

¹³ Aims and Objectives; Criminal Justice System – http://www.cjsonline.gov.uk/the_cjs/aims_and_objectives/index.html

Figure 33 sets out how the Department for Work and Pensions ensure professional standards are maintained through its emphasis on standards assurance. HM Revenue & Customs approach to assuring standards is set out in **Figure 34**.

Figure 33
How the Department for Work and Pensions reviews investigations

The Department operates a number of systems to ensure they are compliant with the criminal justice system:

- investigations and prosecutions are run separately;
- authority to gather intelligence under the *Social Security Act 2001* is only available to a limited number of authorised officers who must have undergone relevant training and hold an appropriate licence;
- a Quality Assurance Framework has been implemented within the Fraud Investigation Service which includes checks on key elements of the intelligence and investigation processes to ensure these comply with instructions.

The Department for Work and Pensions set up the Fraud Investigation Service in 2006 to investigate cases likely to result in a criminal sanction. The Service has developed a Strategy and Planning Support Team structure to improve the standards of fraud investigations and ensure that Learning and Development products meet the changing needs of investigation staff.

The Surveillance Commissioner reports annually on the use of covert methods in investigations and compliance with the *Regulation of Investigatory Powers Act 2000*, *Data Protection Act 1998* and *Human Rights Act 1998*. The results of these assurance checks are used to identify areas for further development and scope for improvement.

The Products and Services Management Division (P&SMD) is responsible for ensuring that the Fraud Procedures and Instructions Manual complies with legislative and operational requirements. This ensures investigators, when engaged in fraud investigations and authorised surveillance, are able to gather sufficient, relevant and reliable evidence, in a legally compliant manner for use in any prosecution or sanction. This guidance was developed in liaison with local authority partners and made available to them. The Department used Home Office guidelines as a basis for their written procedures on the use of surveillance.

Figure 34
The arrangements used by HM Revenue & Customs to review investigation processes

A separate team in HM Revenue & Customs – Criminal Justice and Enforcement Standards – is dedicated to maintaining professional standards in criminal investigation. This team is independent of the Criminal Investigation directorate. Criminal investigation is also subject to review by the Department’s Internal Audit directorate.

External oversight is provided by the HM Inspectors of Constabulary and the Scottish and Northern Ireland inspectors. Complaints about investigations can be made to the Police Complaints Commission, the Ombudsman and the Adjudicator.

Imposing sanctions

“Effective sanctions can do more than simply punish the individual: they have a wider deterrent impact and should also provide an incentive to encourage the non-compliant to return to compliance. Visible sanctions that work can reinforce the perception among compliant taxpayers that the system is fair.”
Simon Norris, Deputy Director, Review of Powers Team, HM Revenue and Customs

3.25 Where investigations find evidence of fraud, departments will usually seek to impose some form of sanction. The purpose is to deter others from carrying out similar types of fraud against the organisation; recover the money defrauded and punish the fraudster by imposing a penalty, such as a fine, or confiscating an asset, or by prosecuting them criminally in the courts. Some departments have published their approach to deter potential fraudsters and ensure that a consistent approach is taken. The NHS Counter Fraud Service imposes parallel sanctions to increase the deterrent effect (**Figure 35**). Departments need to consider whether the level and range of sanctions imposed on fraudsters provide a sufficient deterrent.

Figure 35**Examples of departments' approaches to imposing sanctions**

Where the **Department for Work and Pensions** has sufficient evidence of fraud to take a case to court they will give a formal caution or impose an administrative penalty; or prosecute those involved.

- Cautions are usually aimed at the less serious benefit frauds and those where the overpayment is under £2,000. The offender must admit to the offence, and the amount overpaid must be paid back. (This applies to England and Wales. There are slightly different arrangements in Scotland).
- An administrative penalty is imposed where the value of the fraud is under £2,000. The person must repay the amount overpaid and an administrative penalty of 30 per cent of the amount of the overpayment.
- Whether cases are prosecuted depends on a number of factors. The value of the fraud should be over £2,000, the strength of the evidence should suggest that conviction is likely and prosecution should be in the public interest. Magistrates or the Crown Court decide on the penalty to be imposed if the person is convicted.

The NHS Counter Fraud Service seeks to combine the application of disciplinary, civil and criminal sanctions where fraud is found – to dismiss an employee or suspend or de-register a professional; to obtain civil law orders to freeze assets and recover funds and to seek a criminal prosecution. The approach is set out in “Applying the Appropriate Sanctions Consistently”, published in April 2003 and updated in December 2007. Copies can be obtained from www.cfsms.nhs.uk.

HM Revenue & Customs operates a progressive regime of sanctions against fraud which is aimed at deterring and penalising fraud and evasion through significant financial penalties. Whilst the deterrent threat of prosecution remains, and is applied in the most serious cases, the majority of evaders can be “hit where it hurts most” through financial penalties of up to 100 per cent of the sums being evaded. This approach seeks to match the level of the penalty to the amount of the tax understated, the behaviour giving rise to the understatement of tax and the extent of co-operation by the taxpayer.

Fines and other penalties

3.26 Fines and other penalties imposed on those committing fraud need to be recovered to ensure that they act as a deterrent. Fines and other penalties imposed on those committing fraud need to be recovered to ensure that they act as a deterrent. In 1999 legislation provided for a new civil penalty charge to be imposed where a person wrongly fails to pay any amount in respect of NHS charges or obtains goods or services to which they are not entitled. If the fine is not paid by the due date then a surcharge of 50 per cent of the penalty can be made up to a maximum of £50.

3.27 It is important to monitor progress in recovering the fines and penalties involved, including the enforcement of fines imposed by the courts for convicted fraudsters. Although in such cases it is not the departments that collect the fines, they should consider working with the Ministry of Justice to determine the level of fines actually paid. The extent of re-offending may indicate whether sanctions provide a sufficient deterrent. The Department for Work and Pensions has previously estimated that 9 per cent of those fraudulently claiming Income Support and Jobseeker's Allowance had been caught before. To help combat this recidivism, the Department introduced legislation in 2002 to allow benefit to be stopped for 13 weeks if individuals were convicted of committing benefit fraud twice within the space of three years. The Department extended the linking period for benefit fraud offences from three to five years in the *Welfare Reform Act 2007*. The NHS Counter Fraud Service may take criminal proceedings against patients for serious cases of repeated or persistent fraud. This criminal offence is designed to complement the civil penalty charge and attracts a fine, on conviction of up to £2,500.

3.28 Departments need to be aware of Article 6 (1) of the *Human Rights Act 1998*, which provides for rights to a fair trial, which says, “*In determination of his civil rights and obligations or of any criminal charge against him, everyone is entitled to a fair and public hearing within a reasonable time by an independent and impartial tribunal established by law*”. As a final recourse, someone who has been subject to a fine or other sanction should be allowed to dispute the sanction in either the magistrates or the county court.

Criminal prosecution

3.29 The *Fraud Act 2006*¹⁴ includes three classes of fraud:

- Fraud by false representation;
- Fraud by failing to disclose information;
- Fraud by abuse of position.

In all three classes of fraud, the Act requires that for an offence to have occurred, the person must have acted dishonestly, and that they had to have acted with the intent of making a gain for themselves or anyone else, or inflicting a loss (or risk of a loss) on another. There are also offences of fraud specific to particular departments' activities.

3.30 Preparing cases to the state of proof required for a criminal prosecution can take a long time and involve significant resources. Decisions on whether to refer cases for prosecution may depend on whether:

- there is sufficient evidence to obtain a conviction;
- the case involves a systematic attack on the department's systems and has led to substantial amounts of money being lost;
- there is a history of re-offending;
- professionals such as lawyers and accountants are involved in the fraud;
- prosecution will increase the deterrent effect.

3.31 These factors need to be balanced against the time and cost of bringing a case to court, and the availability of other forms of sanction which may be more appropriate. Some departments have laid down the circumstances in which they will refer cases for prosecution to ensure they take a consistent approach in each case (**Figure 36**). Departments will need to consider whether the number of prosecutions is commensurate with the potential sums at stake in lost revenue, provide a sufficient deterrent and meet the wider public interest in prosecuting significant dishonest conduct.

Figure 36

HM Revenue & Customs normally refer for prosecution the most serious cases of VAT evasion

In April 2005 the **Revenue and Customs Prosecutions Office** was set up, under the superintendence of the Attorney General, as an independent prosecutor to prosecute cases referred to it by HM Revenue & Customs and the Serious Organised Crime Agency within England and Wales. In Scotland, cases are reported for consideration of prosecution to the Crown Office and Procurator Fiscal Service.

Prosecution is an important part of HM Revenue & Customs' armoury to tackle VAT fraud. It refers the most serious cases of evasion for prosecution. Cases are referred where a strong deterrent message is required and the use of other options will not achieve this. However, HM Revenue & Customs may investigate any case of suspected dishonest evasion of VAT with a view to referring the case for prosecution.

Cases are referred for prosecution where HM Revenue & Customs published criteria for criminal investigation may apply. The Revenue and Customs Prosecutions Office will consider whether the evidence is sufficient, whether prosecution is in the public interest and who should be charged and with what offence(s). It follows the Code for Crown Prosecutors, issued by the Director of Public Prosecutions that sets out the general principles Crown Prosecutors should follow when they make decisions on cases. Revenue and Customs Prosecutions lawyers can also provide guidance to the criminal investigators of HM Revenue & Customs and Serious Organised Crime Agency during the investigation and prosecution process.

¹⁴ *Fraud Act 2006* – http://www.opsi.gov.uk/acts/acts2006/pdf/ukpga_20060035_en.pdf

The recovery of money defrauded

“Asset recovery prevents criminal proceeds being reinvested in other forms of crime. By reducing the rewards of crime, it begins to affect the balance of risk and reward, and the prospect of losing profits may deter some from crime. Fundamentally it serves justice, in that nobody should be allowed to continue to profit from crime. The long term purpose of recovering the proceeds of crime is to reduce harm.” *Asset Recovery Action Plan*, Home Office, May 2007

3.32 The means of recovering assets whether in or outside of the UK may be achieved through the criminal process or through the civil courts. Where it is decided to embark on a prosecution then criminal remedies should take priority over civil. Any decision to proceed with a civil action should be taken in consultation with the prosecutor. As part of an investigation, departments may look into the financial affairs of the suspected fraudster to see whether evidence can be provided to the court on the extent of the benefit obtained by the defendant, and to make a confiscation order. Before the suspected person or persons become aware that an investigation is taking place, action may be needed to secure misappropriated funds by a criminal restraint order or seeking a civil injunction.

3.33 Where an organisation seeks to recover stolen monies through the civil courts it will have to prove on a balance of probabilities, that it has cause of action against the defendant. Further the claimant will have to prove the amount taken. If successful the court will then make an order against the defendant requiring him or her to compensate the claimant together with an award of costs in most cases. Legal costs can be high. Organisations will need to consider:

- the amounts stolen and which therefore could be recoverable;
- the prospects of winning the case;
- the value of assets held by the suspected fraudster;
- the likely legal costs;
- whether it will be possible to pursue a civil action whilst a criminal investigation is underway.

3.34 Organisations may be able to recover stolen monies as part of criminal proceedings where the prosecutor secures a compensation order in favour of the victim as part of the offender's sentence. Further information about civil and criminal actions to recover assets can be found on the website of the Serious Organised Crime Agency.

3.35 The powers to deprive criminals of their assets increased substantially as a result of the *Proceeds of Crime Act* 2002. The legislation brought together and strengthened in one Act the drug and non-drug confiscation legislation previously contained in the *Drug Trafficking Act* 1994 and Part VI of the *Criminal Justice Act* 1988. Under the Act, any offence that generates proceeds is capable of attracting criminal confiscation, and the availability of restraint (court freezing of property pending confiscation) is brought forward from the point at which a person is about to be charged to any time from the start of a criminal investigation. The Act established the Assets Recovery Agency to investigate and secure criminal assets. Law enforcement agencies could pass confiscation cases to the Agency for it to apply for restraint, to undertake the confiscation hearing or to enforce confiscation cases. In addition, the Act created a new civil recovery scheme, empowering the Agency to sue in the High Court to recover property derived from crime without the need for anybody to have been convicted of an offence. There is also an option to tax the proceeds of crime where there are reasonable grounds to suspect a person's income, profit or gain was derived from crime.

3.36 The *Serious Crime Act 2007* abolished the Assets Recovery Agency and transferred its civil recovery and taxation powers to the Serious Organised Crime Agency which now undertakes civil recovery and tax investigations in England, Wales and Northern Ireland. The Act also conferred on the Revenue and Customs Prosecutions Office, the Crown Prosecution Service, the Serious Fraud Office and Public Prosecutor Northern Ireland the power to bring civil recovery proceedings in the same way as the Assets Recovery Agency.

3.37 Whilst other agencies are developing their civil recovery capabilities, the Serious Organised Crime Agency is providing support by taking on cases referred to it, where the use of civil recovery and tax powers would be in the public interest. Where a law enforcement agency or prosecution authority has a criminal case which it has been unable to prosecute successfully it can refer the case to the Serious Organised Crime Agency. For a case to be considered for adoption by the Agency recoverable property must have been identified and have an estimated value of at least £10,000; the recoverable property must include property other than cash or negotiable instruments (although cash is recoverable if it is in addition to other property); and there must be evidence of criminal conduct that is supported to the civil standard of proof, that is, on the balance of probabilities. **Figure 37** outlines actions taken by the Department for Work and Pensions to recover assets and **Figure 38** provides an example of Revenue and Customs Prosecutions Office application of criminal confiscation powers.

3.38 The Home Office has recently consulted on proposals to increase dramatically the quantity of criminal assets recovered. Its proposals are set out in the Assets Recovery Action Plan of May 2007.

Figure 37

Action to recover assets and seek criminal compensation

The Department for Work and Pensions has emphasised the punitive, deterrent and disruptive effects of the recovery of assets deemed to be the proceeds of crime and are making use of the new powers of confiscation for offences committed under the *Proceeds of Crime Act 2002*. In 2007-08, the Department obtained 136 confiscation orders, 33 compensation orders and 85 voluntary payments as a direct result of the *Proceeds of Crime* powers. These totalled £7.55 million with a further £54,266 paid in costs to the Department for the confiscation proceedings.

Figure 38

Revenue and Customs Prosecutions Office use of criminal confiscation powers to recover the proceeds of crime

In 2006-07 the Revenue and Customs Prosecutions Office restrained £103.6 million in assets to prevent them being dissipated and obtained 445 confiscation orders worth £55.7 million. The Revenue and Customs Prosecutions Office collected confiscation receipts of £24.2 million at a cost of £2.2 million.

Revenue and Customs Prosecutions Office prosecuted the owner of an accountancy practice in Torquay although he was not a qualified accountant. He took on the affairs of a wealthy local family who had recently paid substantial amounts in Capital Gains Tax on the sale of their business. He submitted a fraudulent claim for the repayment of the Capital Gains Tax on his clients' behalf and forged their signature on a payment authority. He then stole the refund of £300,000 and used it to pay for an extravagant lifestyle. He pleaded guilty to forgery and was sentenced to 30 months' imprisonment and a confiscation order of £370,000 with five years in default.

Evaluating the effectiveness of sanctions

3.39 Evaluating the effectiveness of sanctions is not straightforward, mainly because of the difficulties in assessing the deterrent effect. In broad terms, the deterrent effect of sanctions will be reflected in whether the amount of fraud has reduced, although it is hard to disentangle the effects of sanctions from other action to reduce fraud as well as wider economic effects. Trends in the indicators given below in **Figure 39** can help to determine whether the level of activity may be having a desirable effect. The Department for Work and Pension has carried out a full review of its sanctions regime, which has been in use since 1998. It concluded that the regime was fit for purpose, but that more could be done to increase claimants' awareness of the sanctions imposed on benefit fraudsters.

Figure 39

Examples of indicators

- number of frauds identified;
- number of identified frauds with no sanction imposed;
- number of cases where re-offending has occurred;
- number of formal cautions given;
- number of penalty charges imposed;
- amount raised by imposition of penalty charges;
- number of cases recommended for criminal prosecution;
- number of convictions achieved;
- amount of fraud loss and amount recovered;
- amount of confiscation order and amount recovered;
- amount of assets seized from the fraudsters.

Working with others in tackling fraud

3.40 Individuals and businesses may be committing frauds against more than one government department or agency. Joint working enables departments to identify common threats and pool their knowledge and expertise to investigate fraudsters. Other benefits of working together to tackle fraud are:

- good practice can be shared across departments;
- information can be exchanged more efficiently;
- skills, informal systems and culture are developed across participating departments;
- a more consistent approach from the different departments can be developed;
- the consistency of information provided by customers to different departments can be tested;
- trust and understanding can be built across departments.

Figure 40

Examples of working with others to tackle fraud

HM Revenue & Customs has worked in partnership with the **Gangmasters Licensing Authority** to identify businesses that should be registered for tax. The Gangmasters Licensing Authority regulates businesses that supply labour for agriculture, horticulture, shellfish gathering and food processing and packaging, to protect vulnerable workers from exploitation. During 2006-07 the Authority and HM Revenue & Customs discovered that at least 40 businesses that applied for a licence should also have been registered for VAT. As a result of this cooperation, those businesses have paid an extra

£2 million in VAT, in addition to national insurance contributions and tax for their 6,000 workers, and corporation tax.

HM Revenue and Customs is making use of suspicious activity reports to detect fraud. Under the Money Laundering Regulations organisations are required to make suspicious activity reports to the Serious Organised Crime Agency where they know or suspect that a transaction involves money laundering. In the period April 2004 to the end of March 2007 HM revenue & Customs completed 7,150 investigations involving over £27 million in tax or around £3,800 in each case.



3.41 Joint working arrangements can be set up to share information and data, discuss issues of common interest and carry out research (**Figure 40**). Such arrangements can be covered by a Memorandum of Understanding with the other organisations setting out for example the arrangements for sharing data and carrying out matching and profiling with their data. The sharing of data may be facilitated through data warehouses accessible to the organisations involved. The data warehouse can include data from each organisation and from external sources such as national insurance numbers, driving licences, passport holders and electoral rolls. In a pilot project, HM Revenue & Customs is using specialist computer software to analyse various internal and external information to help identify potential ghosts (people who work in the hidden economy and pay no tax on their earnings) and moonlighters (people who pay tax on certain earnings but fail to declare other sources of income).

3.42 Joint working may also include co-operation on fraud investigations. This enables departments to identify and investigate cases of common interest, avoiding duplication of effort. The *Welfare Reform Act 2007* enables local authorities to investigate suspected frauds on benefits administered by the Department for Work and Pensions. The Department also cooperates with local authorities to identify and jointly investigate cases. There are a number of factors that need to be considered for effective joint working in fraud investigations (**Figure 41**).

Figure 41

Good practice in joint working to investigate external frauds

Aim to establish with the other organisations involved in joint fraud investigations:

- common criteria for selecting which cases to investigate;
- the time scales for investigations;
- agreed procedures for dealing with cases by either the civil route or criminal prosecution;
- the different powers of the departments to investigate and the sanctions that can be used.

GOOD
PRACTICE
GUIDE

Design and Production by NAO Marketing & Communications Team
DG Ref: 8383RA | Printed by Maxim
© National Audit Office 2008



National Audit Office